SECTION II—REMARKS

Claims 26-45 rejected under 35 U.S.C. § 103(a)

The Office Action rejected claims 26-45 under 35 U.S.C. § 103(a) as being unpatentable over Mukherjee et al. in view of U.S. Patent Application Publication No. 2004/0006708 to Cheline ("Cheline") and U.S. Patent Application Publication No. 2004/0255154 to Kwan, et al. ("Kwan"). Applicants respectfully disagree.

The combination of references proposed in the Office Action, specifically, combining the diverse authentication and user authorization mechanisms of Mukherjee with those of Cheline and further with those of Kwan, render Mukherjee "**unsatisfactory for its intended purpose**," in violation of the guidelines set forth under M.P.E.P. § 2143.01(V) and further "**change[s] the principle of operation**" of Mukherjee in violation of the guidelines set forth under M.P.E.P. § 2143.01(IV).

In accordance with M.P.E.P. § 2143.01(V), a "proposed modification [that] would render the prior art invention being modified (e.g., Mukherjee) **unsatisfactory for its intended purpose**," is an improper modification, and as such, "there **is no suggestion or motivation** to make the proposed modification."

Similarly, in accordance with M.P.E.P. § 2143.01(VI), a "proposed modification or combination of the prior art [that] would **change the principle of operation** of the prior art invention being modified" is an improper modification, and as such, "the teachings of the references **are not sufficient** to render the claims *prima facie* obvious."

Overview of each of the respective references:

The Office Action alleges that a combination and modification of three distinct prior art references, Mukherjee, Cheline, and Kwan, renders independent claim 26 obvious. In particular, the Office Action concedes that neither Mukherjee or Cheline disclose "blocking all data packets received at the first port of the packet forwarder," but states that Kwan does disclose the limitation. The Office Action states that it would have been obvious to "**modify the method** disclosed by (the modified combination of) Mukherjee and Cheline to include blocking all data packets," and that this modification would have been motivated to "provid[e] a **first level of security that comprises authentication of the physical (MAC) address of a user device coupled to a port of the network device**."

Such a modification is not possible however, without rendering the modified reference both "unsatisfactory for its intended purpose" and "chang[ing] the principle of operation" of the modified reference," as each Mukherjee, Cheline, and Kwan disclose **different and incompatible** mechanisms for providing authentication of incoming devices or users. Each reference discloses a different type of authentication because each reference sets out to **solve a different problem** than the other, and each focuses on different priorities and capabilities in their respective authentication schemes, and compromise in other areas of their respective authentication schemes.

For example, with reference to Mukherjee specifically, Mukherjee seeks out to provide what is effectively an outsourced P2P-VPN service that users, companies, government organizations, and so forth can utilize to obtain secure communications over publicly accessible network infrastructure **without having to own, operate, or control** the equipment themselves. For example, Mukherjee explains:

> [0014] The present invention provides **peer-to-peer virtual private network (P2P-VPN) services to individual customers**. ... The VISA [and] ... P2P-VPN service [operates] in conjunction with the infrastructure and **a public network**.
>
> [0015] The P2P-VPN service allows individual customers to request[] the P2P-VPN service ... **for a monthly fee** (similar to customer phone service). Alternatively, the individual customer can order such service on an **on-demand basis**. It is noted that the P2P-VPN services of the present invention differ from current P2P-VPN services in that **any individual** who is not affiliated with an enterprise, such as a corporation, government body, or other organization environment, **may also receive P2P-VPN services**.

Thus, as noted above, Mukherjee sets out to provide P2P-VPN services to customers as a service, so that those customers do not have to own, operate, or otherwise manage the complex infrastructure required to support P2P-VPN services. In that vein, Mukherjee contemplates and describes an authentication mechanism by which "**any individual ... may also receive P2P-VPN services**." For example:

> [0047] At step 310, the user group is assigned a network access identifier (NAI). ... a user simply buys (subscribes to) the services from the service provider 102, where the required infrastructure exists. Furthermore, by providing an NAI for the group, **the users may easily connect to the P2P-VPN network from anywhere in the world, as well as join and leave the VPN at any time (i.e., 24x7 service) from any end-user device** 130 using wireless or wired access networks 120.
>
> [0048] At optional step 312, the service provider will **register the names of members who may participate** in the P2P-VPN services. ... .

Thus, Mukherjee has selected an authentication mechanism by which "any end-user device" may connect and utilized the provided service "from anywhere" and "at any time," so long as the service provider has "register[ed] the names of [the] members" as those who are authorized to "participate in the P2P-VPN service[]."

As Mukherjee makes exceedingly clear, the authentication mechanism described allows for as great as flexibility (e.g., "from anywhere ... at any time ... from any end-user device") for potential customers to become paying subscribers as possible, while still exerting authentication authority over potential users of the service by requiring that they be registered by the service provider.

The Office Action, at page 4, last paragraph, proposes to combine Mukherjee's invention with the stringent authentication regime set forth by Kwan. In particular, the Office Action states:

> ... it would have been obvious ... to modify the method disclosed by Mukherjee ... to provide a network device that implements a **multiple key, multiple tiered system and method for controlling access** to a data communications network in both a single host and multi-host environment by providing a **first level of security** that comprises authentication of the physical (MAC) address of a user device coupled to a port of the network device, such as a network switch, a **second level of security** that comprises authentication of a user of the user device if the first level of security is passed, such as authentication in accordance with the IEEE 802.1x standard, and a **third level of security** that comprises dynamic assignment of the port to a particular VLAN based on the identity of the user if the second level of security is passed as suggested by Kwan in [paragraph] (0009).

Kwan no doubt proposes a complex gauntlet of security and authentication mechanisms for "controlling access to a data communications network." However, it is precisely the complex and multi-tiered security architecture that makes Kwan incompatible with Mukherjee, so much so that the proposed modification renders Mukherjee "unsatisfactory" for its intended purpose and further "change[s] the principle of operation" of Mukherjee.

For instance, rather than allowing users to "easily connect ... from **anywhere** in the world ... at **any time** ... from **any end-user device**," as expressly described and intended by

Mukherjee (refer to paragraph 48), the proposed modification set forth in the Office Action requires that, in accordance with Kwan, the users only access the proffered P2P-VPN services by utilizing a specially adapted hardware device, such as an end-user device configured with a uniquely enumerated "secure MAC address." For example, Kwan describes one of his many authentication requirements as follows:

> **[0042]** As discussed above, network switch 102 is adapted to **perform a physical (MAC) address authentication** of a user device that is coupled to one of its ports. In particular, network switch 102 is adapted to store a **limited number of "secure" MAC addresses for each port**. A port will forward only packets with source MAC addresses that **match its secure addresses**. ... [If] a packet ha[s] a source MAC address that is different from any of the secure learned addresses, a **security violation occurs**.

Thus, the Office Action proposes a modification wherein Mukherjee **does not** allow users to "easily connect ... from **anywhere** in the world ... at **any time** ... from **any end-user device**," as expressly described, so long as the name of the user is registered as being allowed to participate. Instead, in accordance with the proposed modification of Kwan, Mukherjee would require that users may only connect if they are registered and are further configured with a "secure MAC address" that is then further matched up to a specific "port," otherwise a "security violation occurs."

Further still, the modification proposed by the Office Action requires that, in accordance with Kwan, the user be further "associated with a VLAN supported by the switch." Kwan describes this further security requirement as follows:

> **[0039]** At step 316, network switch 102 determines **whether or not the user is associated with a VLAN supported by the switch**. ... .
>
> * * *
>
> **[0071]** If network switch 102 **does not support the VLAN** identified by the VLAN ID, network switch 102 assigns the port to

> a port default VLAN (or the port remains assigned to the port default VLAN, if already so configured) and **all traffic on the port is blocked** ***except*** for the reception or transmission of 802.1x control packets ... .

Thus, the modification of Mukherjee with the stringent security regime of Kwan requires that not only Mukherjee limit its services to those end user devices which are specially adapted and configured with a "secure MAC address" that is specifically enumerated and associated with a particular "port" of Kwan, but that Mukherjee further limit still the availability of its P2P-VPN services to those user devices that are "associated with a VLAN **supported** by the switch," else the user's non-control traffic will be blocked by the switch.

Applicants respectfully submit that combining Mukherjee with the disclosure of Kwan and in particular, modifying Mukherjee from a system that, as described, expressly allows users to "easily connect ... from **anywhere** in the world ... at **any time** ... from **any end-user device**," so long as the user is registered, to a system that instead restricts the availability of its P2P-VPN services to those users that 1) contain a specially adapted and configured "**secure MAC address**" that is specifically enumerated and matching a particular "port" to which the user connects, and are further 2) associated with a VLAN **supported** by the switch renders Mukherjee "**unsatisfactory** for its intended purpose," and further "**change[s] the principle of operation**" of Mukherjee.

Mukherjee has selected an authentication regime which does not require special hardware requirements or capabilities from the hardware devices utilized by its subscribing customers, presumably, to ensure that its P2P-VPN services are available to as many potential customers as possible. Modifying Mukherjee to require the specialized hardware capabilities of user devices as set forth by Kwan, and thus severely limiting the very customer base to which Mukherjee sets

out to provide P2P-VPN services undermines the expressly stated and intended purpose of Mukherjee and severely alters the manner in which Mukherjee operates, thus changing the principle of operation of the reference.

Because the combination of Mukherjee, Cheline, and Kwan, as set forth by the Office Action, is an improper combination and modification under M.P.E.P. § 2143.01(V), and M.P.E.P. § 2143.01(VI), and is insufficient to establish a *prima facie* case of obviousness, Applicants respectfully request the Examiner to withdraw the rejection to claims 26-45.

The cited references fail to disclose at least one limitation:

Further to the above discussion with respect claims 26-45 rejected under 35 U.S.C. § 103, Applicants respectfully submit that Mukherjee, Cheline, and Kwan whether considered alone or in combination, nevertheless fail to disclose at least one limitation claimed by Applicants.

In particular, Applicants recite in independent claim 26, "**blocking all data packets** received at the first port of the packet forwarder from accessing the network."

The Office Action concedes that both Mukherjee and Cheline fail to disclose the limitation, stating at page 4, last paragraph, "Mukherjee and Cheline do not explicitly disclose blocking all data packets received at the first port ... ." The Office Action alleges, however, that Kwan does disclose the limitation, referring specifically to Kwan at paragraphs 38, 39, and 71, which state in pertinent part:

> [0038] ... As shown at step 312, **if the user is not valid,** then the security protocol proceeds to step 314, in which network switch 102 **blocks all traffic on the port *except* for the reception or transmission of 802.1x control packets on the port**. ... .
>
> [0039] At step 316 ... the port to which user device 108 is coupled is (or remains) assigned to a port default VLAN and **all traffic on the port is blocked *except* for the reception or**

transmission of 802.1x control packets, as shown at step 318. ...

* * *

[0071] If network switch 102 does not support the VLAN ... **all traffic on the port is blocked *except* for the reception or transmission of 802.1x control packets**, as shown at step 526. ...

Thus, as expressly described, Kwan "blocks all traffic ... ***except*** for the reception or transmission of 801.1x control packets." Therefore, stated differently, Kwan does not block **all** packets, but rather blocks **most** packets, as the "reception and transmission of 801.1x control packets" are indeed still packets.

Applicants thus respectfully submit that the mechanism disclosed by Kwan, which blocks **most** packets, and in particular, "all traffic ... ***except*** for the reception or transmission of 801.1x control packets," is not the same as "**blocking all data packets** received at the first port of the packet forwarder from accessing the network," as Applicants recite in independent claim 26.

Of important note, Applicants do not recite that the "reception or transmission of 801.1x control packets" are exempted from the "blocking **all data packets**," limitation claimed.

Because "blocking **all data packets**," as claimed by Applicants is different than blocking **most** data packets, with the **exception** of "the reception or transmission of 802.1x control packets," as described by Kwan, Applicants respectfully submit that independent claim 26 as previously presented is not obvious in light of the combination of Mukherjee, Cheline, and Kwan, and is in condition for allowance. Applicants further submit that independent claims 35 and 40, which recite similar limitations as well as those claims which depend upon independent claims 26, 35, and 40 are patentable over the references and in condition for allowance for at least the same reasons.

Accordingly, Applicants respectfully request the Examiner to withdraw the rejection to claims 26-45.

SECTION III—CONCLUSION

Given the above remarks, all claims pending in the application are in condition for allowance. If the undersigned attorney has overlooked subject matter in any of the cited references that is relevant to allowance of the claims, the Examiner is requested to specifically point out where such subject matter may be found. Further, if there are any informalities or questions that can be addressed via telephone, the Examiner is encouraged to contact the undersigned attorney at (503) 439-8778.

Charge Deposit Account

Please charge our Deposit Account No. 02-2666 for any additional fee(s) that may be due in this matter, and please credit the same deposit account for any overpayment.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

/Gregory. D Caldwell/ Date: April 3, 2009
Gregory D. Caldwell
Registration No. 39,926
Attorney for Applicants

Blakely, Sokoloff, Taylor & Zafman LLP
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
Telephone: (503) 439-8778
Facsimile: (503) 439-6073